

Mathematical Journal of Okayama University

Volume 28, Issue 1

1986

Article 1

JANUARY 1986

A characterization of quadratic residue codes

Noboru Ito*

*Konan University

Copyright ©1986 by the authors. *Mathematical Journal of Okayama University* is produced by The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

A CHARACTERIZATION OF QUADRATIC RESIDUE CODES

To Bertram Huppert on his 60th birthday

NOBORU ITO

1. Introduction. Let n be an odd integer > 1 , and V the space of row vectors of size n over $\text{GF}(2)$. Let $u = (u_0, u_1, \dots, u_{n-1})$ and $v = (v_0, v_1, \dots, v_{n-1})$ be vectors of V . Then the weight of u , denoted by $\text{wt}(u)$, is the number of i 's such that $u_i = 1$, $0 \leq i \leq n-1$, and the distance between u and v , denoted by $d(u, v)$, is the number of i 's such that $u_i \neq v_i$, $0 \leq i \leq n-1$. Obviously, $d(u, v) = \text{wt}(u-v)$.

(V, d) is a metric space. An automorphism τ of (V, d) is an automorphism of V preserving d , and so τ may be regarded as a permutation on n coordinate positions of vectors. Thus the automorphism group of (V, d) is the symmetric group S_n of all permutations on n coordinate positions of vectors.

A subspace C of V is called a binary code of length n . An automorphism τ of (V, d) such that $C\tau = C$ is called an automorphism of C . The set of all automorphisms of C forms a subgroup $G(C)$ of S_n called the automorphism group of C .

C is called cyclic if $G(C)$ contains an n -cycle s . Usually s is taken as the cyclic shift $(0, 1, \dots, n-1)$, and then V and u are identified with the ring $R_n = \text{GF}(2)[x]/(x^n-1)$ and a polynomial $u_0 + u_1x + \dots + u_{n-1}x^{n-1} \pmod{(x^n-1)}$ respectively. Under this circumstance a cyclic code C becomes an ideal of R_n and vice versa.

Let Z be the ring of integers and $Z_n = Z/(n)$. Then Z_n may be regarded as the set of n coordinate positions of vectors. Let a be an integer relatively prime to n . Let $\langle a \rangle$ be a multiplicative subgroup of Z_n generated by a . A multiplicative coset $\langle a \rangle i$, $i \in Z_n$, of Z_n with respect to $\langle a \rangle$ is called a cyclotomic coset with respect to a . Obviously, $\langle a \rangle 0 = \{0\}$. Further let μ_a be a permutation on Z_n defined by $i\mu_a = ia$, $i \in Z_n$.

Now R_n may be regarded as the group algebra over $\text{GF}(2)$ of a cyclic group of order n . Since n is odd, R_n is semisimple and a cyclic code C is generated by an idempotent e . Let $e = \sum_{i \in S} x^i$, where S is a subset of Z_n . We notice that 2 is relatively prime to n . Then since e is an idempotent, $S\mu_2 = S$. Namely S is a union of cyclotomic cosets with respect to 2.

A partition of $Z_n - \{0\}$ into two subsets S and T , $Z_n - \{0\} = S \cup T$ and

$S \cap T = \emptyset$, is called a splitting of Z_n if S and T are unions of cyclotomic cosets with respect to 2 and if there exists an integer a relatively prime to n such that $T = S\mu_a$. Now let C be a cyclic code and e the idempotent of C , $e = \sum_{i \in U} x^i$, where U is a subset of Z_n . If $U = S, \{0\} \cup S, T$ or $\{0\} \cup T$, then C is called duadic (See [2]).

If $n = p$ is a prime such that 2 is a quadratic residue mod p , then $Z_n - \{0\} = Q \cup N$, where Q and N denote the sets of quadratic residues and non-residues mod. p respectively, is a splitting of Z_p and the corresponding duadic codes are called quadratic residue codes. Thus duadic codes are generalization of quadratic residue codes.

Let u be a vector of length n . Then a vector \bar{u} of length $n+1$ defined by $\bar{u} = (u, \overline{\text{wt}(u)})$, where $\overline{\text{wt}(u)} = \text{wt}(u) \pmod{2}$, is called the extension of u by an overall parity check. If C is a code of length n and $\bar{C} = \{\bar{u}, u \in C\}$, then \bar{C} is called the extension of C .

Now the purpose of the present paper is to prove the following theorem.

Theorem. *Let C be a duadic code of length n and \bar{C} the extension of C . If the automorphism group $G(\bar{C})$ of \bar{C} is transitive on the set $\Omega = Z_n \cup \{\infty\}$ of $n+1$ coordinates positions and contains no regular normal subgroup, then n equals a prime p and C is equivalent to a quadratic residue code of length p .*

2. Proof of Theorem. For the proof we use the following facts on duadic codes. For these see [2].

Fact 1. Any prime factor of n is congruent to $\pm 1 \pmod{8}$.

Fact 2. Let $d(C) = \min_{0 \neq u \in C} |\text{wt}(u)|$. $d(C)$ is called the minimum weight of C . For duadic C $d(C) \geq 3$.

Fact 3. The automorphism group $G(C)$ of C contains an n -cycle (which is clear from the definition of C).

We may assume that $G(C)$ is the stabilizer of ∞ in $G(\bar{C})$, the automorphism group of \bar{C} . So by Fact 3 $G(\bar{C})$ is 2-transitive on Ω . All 2-transitive groups without regular normal subgroups are known ([1]). So, in order to prove the theorem, we check the list one by one.

(i) By Fact 1 we can eliminate immediately 2-transitive groups of sporadic and of twisted type of even degrees. Namely the Higman-Sims group has degree 176, the Conway group has degree 276, and Ree groups have degrees q^3+1 , where $q = 3^{2\lambda+1}$ with $\lambda \geq 1$.

(ii) If $G(\bar{C})$ contains the alternating group of degree $n+1$, then $G(\bar{C})$

contains all 3-cycles. Then it is easy to see that C contains a vector of weight 2 against Fact 2.

(iii) If $G(C)$ is a 2-transitive group of unitary type, then $n+1 = q^3+1$, where $q = p^s$ is odd. Let s_p be the p -part of s . Then the order of a Sylow p -subgroup P equals fp^{3s} , where f is a divisor of s_p . If P contains an n -cycle σ , then σ^f belongs to a Sylow p -subgroup of the projective special unitary group $\text{PSU}(3, q^2)$ which has exponent p . Since the order of σ^f equals p^{3s}/f , we have a contradiction.

(iv) Now assume that $G(\bar{C})$ is a 2-transitive group of symplectic type. Then we have that $n+1 = 2^{\lambda-1}(2^\lambda+1)$ or $n+1 = 2^{\lambda-1}(2^\lambda-1)$, where $\lambda \geq 3$. In the first case, $n = (2^\lambda-1)(2^{\lambda-1}+1)$. If λ is even, then $n \equiv 0 \pmod{3}$. If $\lambda \equiv 3 \pmod{4}$, then $n \equiv 0 \pmod{5}$. So by Fact 1 we have that $\lambda \equiv 1 \pmod{4}$. In the second case, $n = (2^\lambda+1)(2^{\lambda-1}-1)$. Similarly as above we obtain that $\lambda \equiv 0 \pmod{4}$. By Fact 3 $G(C)$ contains an n -cycle Z . Since n is odd, the matrix Z of degree 2λ over $\text{GF}(2)$ has an eigenvalue α which is a primitive n -th root of unity over $\text{GF}(2)$. Let $\text{GF}(2^s) = \text{GF}(2)(\alpha)$.

Here and below we use the following theorem of Zsigmondy (For a proof see [3]): Let a and b be positive integers greater than 1. Then there exists a prime number p such that b equals the order of a modulo p . Exceptions occur only when $a = 2$ and $b = 6$, and a is a Mersenne prime and $b = 2$.

Now in our first case there exist two primes p_1 and p_2 such that λ and $2(\lambda-1)$ are the orders of 2 modulo p_1 and modulo p_2 respectively. So we have that $s > 2\lambda$. This is a contradiction. Similarly in our second case there exist two primes p_1 and p_2 such that 2λ and $\lambda-1$ are the orders of 2 modulo p_1 and modulo p_2 respectively. So we have again that $s > 2\lambda$. This is a contradiction.

(v) Finally we assume that $G(\bar{C})$ is a 2-transitive group of linear type. So Ω may be identified with the set of points of the projective geometry of dimension $\lambda-1$ over $\text{GF}(q)$ and we have that $\text{PSL}(\lambda, q) \subseteq G(\bar{C}) \subseteq \text{P}\Gamma\text{L}(\lambda, q)$, where $\text{PSL}(\lambda, q)$ and $\text{P}\Gamma\text{L}(\lambda, q)$ are the projective special linear group and the projective semi-linear group of degree λ over $\text{GF}(q)$ respectively. Furthermore we have that $n+1 = (q^\lambda-1)/(q-1)$ and $n = (q^{\lambda-1}-1)/(q-1)$. Since $n+1$ is even, $q = p^s$, where p is a prime, is odd and λ is even.

Let us assume that $\lambda \geq 4$. Let $\text{PGL}(\lambda, q)$ denote the projective general linear group of degree λ over $\text{GF}(q)$. Let $u = \langle (1, 0, \dots, 0) \rangle$ and $v = \langle (0, 1, 0, \dots, 0) \rangle$ be two points of Ω . By Fact 3 the stabilizer $(\text{P}\Gamma\text{L}(\lambda, q))_u$ of u in $\text{P}\Gamma\text{L}(\lambda, q)$ contains an n -cycle Z so that $(\text{P}\Gamma\text{L}(\lambda, q))_u = (\text{P}\Gamma\text{L}(\lambda, q))_{uv}$

$\langle Z \rangle$ and $(\text{PFL}(\lambda, q))_{u,v} \cap \langle Z \rangle = \langle 1 \rangle$, where $(\text{PFL}(\lambda, q))_{u,v}$ is the stabilizer of u and v in $\text{PFL}(\lambda, q)$. Now $Z = Z_g Z_a$, where Z_g belongs to $(\text{PGL}(\lambda, q))_u$ and Z_a is a field automorphism. Let f be the order of Z_a . Then f is a divisor of s and Z^f belongs to $\text{PGL}(\lambda, q)$ and has order n/f . Clearly the p -part of n/f is greater than 1.

Since p is odd and $\lambda \geq 4$, by the above theorem of Zsigmondy there exists a prime number t such that $s(\lambda-1)$ is the order of p modulo t . Then $s(\lambda-1)$ is a divisor of $t-1$, and hence n/f is divisible by t .

Let A be an element of $\text{GL}(\lambda, q)$, the general linear group of degree λ over $\text{GF}(q)$, corresponding to Z^f . Then $A = PS = SP$, where P and S denote the p -part and prime to p -part of A respectively. Then S has the form

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ & a_2 & & \\ & & S_1 & \\ & \vdots & & \\ & & & a_{\lambda-1} \end{pmatrix}, \text{ where } a_i \in \text{GF}(q), 1 \leq i \leq \lambda \text{ and } S_1 \text{ has degree } \lambda-1.$$

Since the order of S is divisible by t , the eigenvalues of S_1 , and hence of S , are all distinct. In fact, if $\lambda (\neq 1)$ is an eigenvalue of S_1 then λ^{q^i} , $1 \leq i \leq \lambda-1$, are eigenvalues of S_1 and they are distinct. Now since P commute with S , P must be diagonalizable. Since P is a p -element, then $P = I$, the identity. This is a contradiction. Thus we obtain that $\lambda = 2$.

Let s_p be the p -part of s . Then a Sylow p -subgroup of $\text{PFL}(2, q)$ has order $s_p p^s$, and a Sylow p -subgroup of $\text{PGL}(2, q)$ is elementary Abelian of order p^s . Since $s_p p \langle p^s \text{ if } s \rangle 1$, Fact 3 implies that $s = 1$. Now we get the theorem by Theorem 6 of [2].

Remark. For $n = 23$ there exists the famous Mathieu group M_{23} which is 4- and hence 2-transitive of sporadic type and the corresponding also famous Golay code. However, the Golay code is equivalent to a quadratic residue code.

REFERENCES

- [1] P. J. CAMERON : Finite permutation group and finite simple group, Bull. London Math. Soc. 13 (1981), 1-22.
- [2] J. LEON, J. M. MASLEY and V. PLESS : Duadic code. IEEE Trans. on Inform. Theory, it-30 (1984), 709-714.
- [3] L. RÉDEI : Über die algebraischzahlentheoretische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy, Acta Sci. Math. Szeged 19 (1958), 98-126.

A CHARACTERIZATION OF QUADRATIC RESIDUE CODES

5

DEPARTMENT OF APPLIED MATHEMATICS

KONAN UNIVERSITY,

KOBE, JAPAN 658

(Received April 10, 1986)